NTT DATA
Global IT Innovator

Information Security Report 2014

NTT DATA Corporation

Corporate Philosophy

(Mission of the NTT DATA Group)

NTT DATA Group utilizes information technology to create new paradigms and values, contributing to the achievement of a more affluent and harmonious society.

Applicable period and timing of this report

- This report applies to all information covered by the NTT DATA Group.
- This report applies to information security initiatives current at the end of December 2013 unless otherwise noted.

Scope of this report

NTT DATA Group (225 companies, including NTT DATA Corporation)
* Current as of December 31, 2013

Department in charge

NTT DATA Corporation
Information Security Office, Quality Assurance Department

Inquiries

NTT DATA Corporation
Information Security Office,
Quality Assurance Department
Toyosu Center Building Annex
3-3-9, Koto-ku, Tokyo 135-8671
TEL: +81 50 5546 2545
URL: http://www.nttdata.co.jp/

CONTENTS

Message from the CISO

Striving to bring customer visions and ideals to reality

Information security for building a safe and secure ecosystem

Markets have been changing drastically in recent years. There seems to be a shift from new technology-driven markets built on emerging technologies, to economics-driven markets seeking the economic effects of value after technologies have matured, and finally to sensibility-driven markets with a focus on providing an objective satisfaction and level of service, rather than just cost-effectiveness alone. And instead of simply incorporating brand new technologies, there also lies the need to be proactive in identifying potential customer needs by analyzing various types of data to see exactly what the customer wants.

Customers now seem to be shifting away from smartphones, tablet devices, cloud services or social networking services as the phrase “big data” is gaining momentum around the world in recent years. While potential needs can be visualized by utilizing this big data, there are also concerns about ensuring the protection of personal information when securely storing and analyzing such vast quantities of personal data. With the enactment of the My Number Act, reviews to ISO/IEC27001 and OECD privacy guidelines, these issues need to be addressed by protecting personal information and personal data, and changing developing or operating standards for security management systems. These are all having a major impact on business. Meanwhile, cyber-attacks took the form of targeted attacks in 2012, however 2013 saw new forms of attacks such as drive-by downloads. There is the need to accurately identify constantly evolving situations.

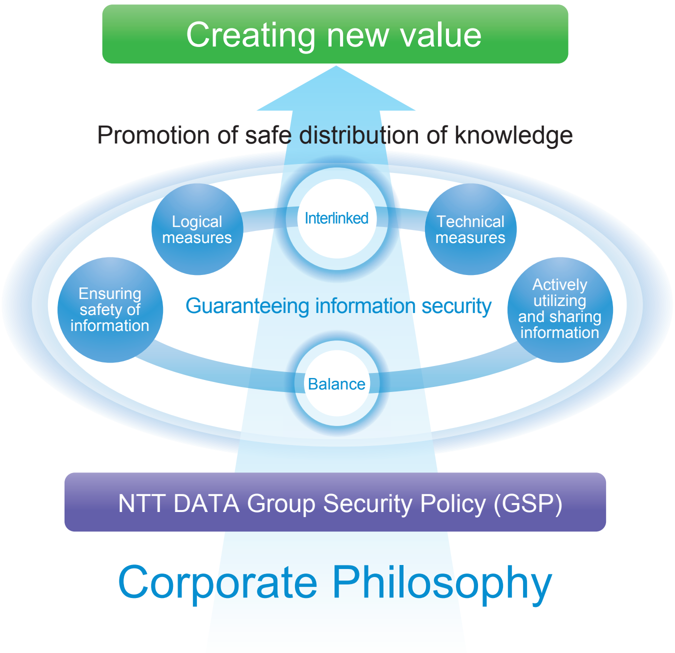
NTT DATA is striving to bring customer visions and ideals to reality by building an ecosystem using advanced IT. To achieve this, developing a safe and secure information-oriented society will be essential. The information security report first issued in 2008 is now in its fourth edition, and outlines the specific measures that NTT DATA is taking for implementing information security activities to develop a safe and secure ecosystem. I would be highly delighted if stakeholders reading through this report find it useful in one way or another.

NTT DATA Corporation
Representative Director and Executive Vice President CISO

Satoshi Kurishima

NTT DATA Group information security policies

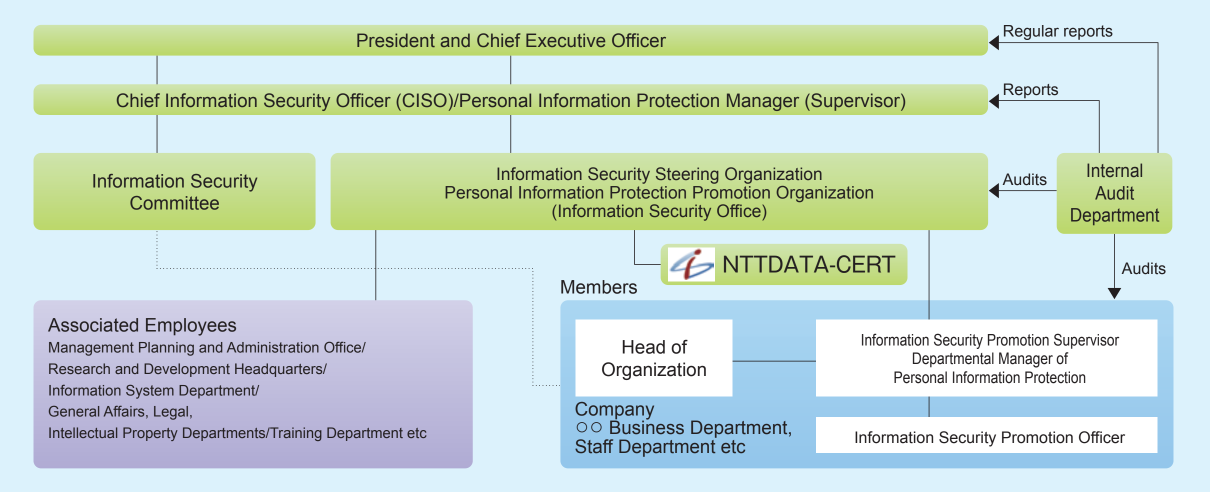
By maintaining an appropriate balance between ensuring safety of information and actively utilizing and sharing information, the NTT DATA Group applies its knowledge throughout the entire group and provide brand new value to customers.
Both logical measures covering the development of rules and providing training and educational activities related to information security, and technical measures for preventing leakages of information or the installation of thin-client PCs are required for adequately ensuring safety of information and actively utilizing and sharing information.


Creating new value
Promotion of safe distribution of knowledge
Logical measures
Interlinked
Technical measures
Ensuring safety of information
Guaranteeing information security
Actively utilizing and sharing information
Balance
NTT DATA Group Security Policy (GSP)
Corporate Philosophy

Development of “Information Security Policy” and “Personal Information Protection Policy”

NTT DATA is fully aware that leakage or unauthorized use of information due to security breaches can lead to major problems, and has focused on initiatives related to information security management from an early stage. More specifically, the "Information Security Policy" was developed in December 1998 with the aim of handling information assets appropriately, and ensuring the utmost information security.
The protection of personal information has long been identified as a factor requiring the highest level of priority, and has been assigned as a core activity of corporate management. In addition to establishing the "Personal Information Protection Policy" in July 2001, internal compliance regulations have been set to ensure that personal information is handled appropriately. The Personal Information Protection Policy and internal compliance regulations are reviewed and improved regularly to meet constant advances being made to information technology and changes in social conditions.

■NTT DATA Information Security, Personal Information Protection Activity Systems


President and Chief Executive Officer
Regular reports
Chief Information Security Officer (CISO)/Personal Information Protection Manager (Supervisor)
Reports
Information Security Committee
Information Security Steering Organization
Personal Information Protection Promotion Organization
(Information Security Office)
Audits
Internal Audit Department
NTTDATA-CERT
Members
Audits
Associated Employees
Management Planning and Administration Office/
Research and Development Headquarters/
Information System Department/
General Affairs, Legal,
Intellectual Property Departments/Training Department etc
Head of Organization
Information Security Promotion Supervisor
Departmental Manager of
Personal Information Protection
Company
○○ Business Department,
Staff Department etc
Information Security Promotion Officer

Information security throughout the entire group

Standardizing key management policies and rules is essential, even at overseas offices, to ensure group and global management. The same concept applies to information security.

The NTT DATA Group developed standardized information security rules called "NTT DATA Group Security Policy (GSP)" in April 2008. Each company within the group has defined its own information security policy based on this GSP to suit the size and type of business of each particular company.

GSP also defines rules on how to handle information. This has allowed the entire NTT DATA Group to handle information safely.

Various systems have been designed and organized, such as a portal site that can be accessed by group employees, including those stationed overseas (Global Internal Portal (GIP)), a group-wide virtual private network on the internet (GWNet), a file transfer system (ETRANPOT), and a document management system (Docφ), as part of an information distribution infrastructure for sharing electronic information throughout the group safely and efficiently.

A technical information knowledge bank (Solution Warehouse®, TeSS) designed to share knowledge between all group employees, encourages information to be utilized and shared safely, and serves to increase the competitive prowess of the entire group.

■Example of Information Distribution Infrastructure

Global Internal Portal (GIP)

Portal site that can be accessed by employees of the NTT DATA Group, including those stationed overseas. This allows sharing of information common to the global group, and provides support for global collaboration activities.

ETRANPOT

System for transferring files securely between the NTT DATA, NTT DATA Group companies and customers. Files cannot be stored for longer than a set period of time.

Docφ

The file-sharing system for use between NTT DATA, NTT DATA Group and contracted companies. Also allows access rights and version management.

Solution Warehouse® / TeSS

Solution Warehouse®: NTT DATA Group technical information database.

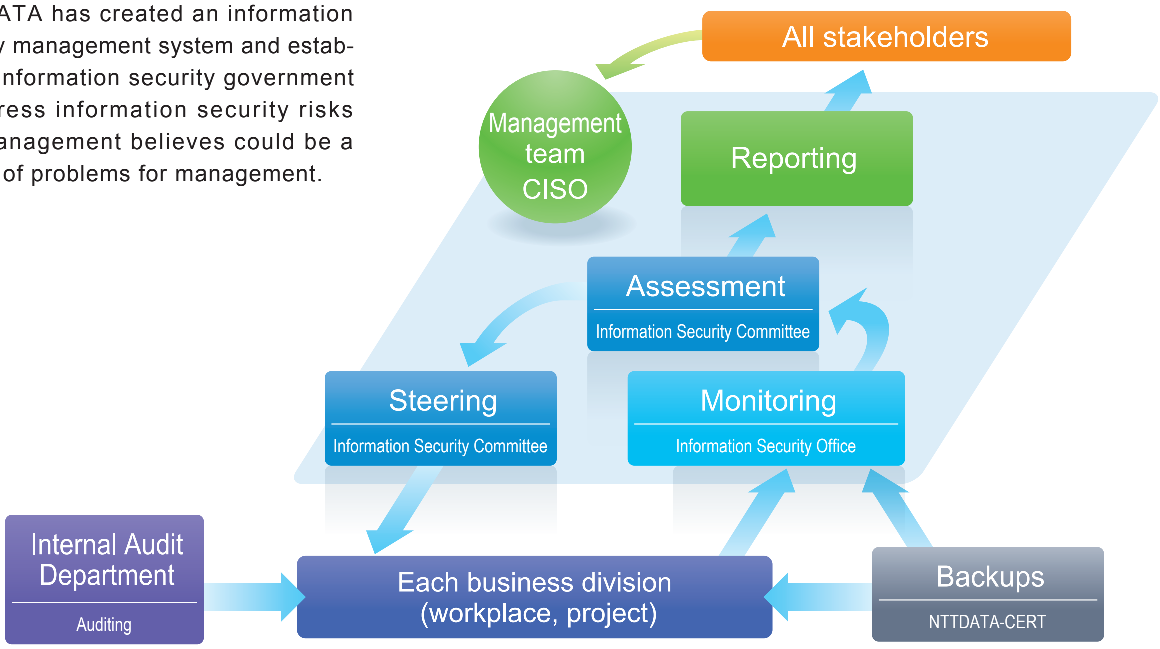
TeSS: contact point for technical inquiries, and associated database.

Know-how is shared and utilized between the group.

NTT DATA information security management system

Establishing information security governance

NTT DATA has created an information security management system and established information security government to address information security risks that management believes could be a source of problems for management.


All stakeholders
Management team CISO
Reporting
Assessment
Information Security Committee
Steering
Information Security Committee
Monitoring
Information Security Office
Internal Audit Department
Auditing
Each business division (workplace, project)
Backups
NTTDATA-CERT

Steering — Information Security Committee

The Information Security Committee is overseen by the Representative Director and Executive Vice President and CISO (Chief Information Security Officer), and held regularly with the managers of each department as members (held a total of 60 times to December 2013).

The Information Security Committee develops information security strategies for the NTT DATA Group with the aim minimizing information security risks, and ensuring safe utilization and sharing of information.

Monitoring — Information Security Office

Established as the special group for implementing information security activities throughout the NTT DATA Group.

This group conducts individual information security activities based on information security strategies, as well as monitoring of the implementation state of each information security activity.

Assessment

Information Security Committee

Information security implementation activities for this fiscal year are based on information security strategies, and are assessed as a whole with monitoring information of each activity, the results of internal audits and other factors. Each activity is reviewed based on the results of the assessment, and proposals are made for new information security strategies.

Auditing

Internal Audit Department

The Internal Audit Department at NTT DATA conducts internal auditing related to information security.

This involves information security audits of each business division from a perspective that is completely independent of business procedures.

Results of audits are relayed to the Information Security Office, and improvements or reviews of systems or activities are implemented whenever required.

Reporting

The NTT DATA Group identifies all customers, shareholders and investors, clients, and employees and their families as stakeholders, and discloses the appropriate information at the appropriate time to fulfill its role of social responsibility as a quality corporate citizen.

The needs of shareholders and investors are carefully attended to by the Investor Relations and Finance Office, the general public, and employees and their families are informed with mass communication via the Public Relations Department, and customers carefully attended to by employees within the Sales Department.

The NTT DATA Group considers taking proactive efforts for establishing information security as one form of social responsibility, and the first information security report as a system integrator was created and released in 2008 to stakeholders.

Backups

NTTDATA-CERT

Established in the Information Security Office and operates as the Special NTT DATA Group Security Incident Response Team (CSIRT)*

Collects and analyzes information, and devises the appropriate response for preventing security incidents from occurring. Provides emergency response in the event that a security incident does occur.

* Note: CSIRT (Computer Security Incident Response Team) is an incident response team comprised of security specialists. The team collects and analyzes information on security incidents, security-related technologies and vulnerabilities, and conducts activities for effective response and training.

Review of details outlined in the 2012 Information Security Report

Reports for all stakeholders

NTT DATA released Japan's first information security report as a system integrator in 2008. This report is the fourth time it has been released.

The 2012 Information Security Report outlines the results of implemented initiatives for information security strategies disclosed to stakeholders by NTT DATA.

Efforts raised in the Information Security Report

Initiatives for information security strategies listed in the previous information security report are as follows.

■Three information security strategies and implementation reports

Information Security Strategies	Implementation Results
Strategy 1 Increasing driving power of information security of group companies overseas	Monitoring had previously targeted group companies in Japan, however was increased to also cover companies overseas from 2011. The state of information security operation has been collected every quarter to provide advice on improvements, as well as validity assessments. The Information Security Office visited eight companies overseas (and five in Japan) to obtain more details on problems or issues that they faced, and also provided on-the-spot advice and looked into further countermeasures. Efforts have also been made into expanding the scope of information security training, with IBT training for GSP conducted in three languages (Japanese, English, and Chinese). The level of awareness of security was determined by measuring the effects after training was conducted. The training has been completed by 20,989 employees from 83 companies worldwide. Training materials for the GSP internal auditor training were created in three languages, with 229 employees from 66 companies worldwide taking part in what helped improve auditing work at each company. Lecturers were dispatched to four new companies overseas that joined the group, to provide literacy training for acquiring the minimum required knowledge as employees of the NTT DATA Group.
Strategy 2 Ensuring basic security behavior	An “Advisory Report” has been created that assesses the state of implementation of information security for each organization, at each business division within NTT DATA as well as group companies. A tour was also conducted for seven organizations within the company and four groups companies to get them recognize their problems assessed in the report. The “7 Wise Conditions for Basic Security Activities” has been conducted twice within the company as case studies, as well as “Information Security ABCD Operations” organized twice as case studies. Information security workshops have also been held five times. An Improvement Month on the theme of Information Security has been arranged once per year, where training for targeted cyber-attacks and tools for preventing incorrect email transmissions are provided. IBT (e-learning) for information security and the protection of personal information has also been conducted once per year.
Strategy 3 Security contributing to management	Operation rules have been formulated within NTT DATA to ensure that social media is used safely for business. The “NTT DATA Social Media Policy” and “Official Account” have been uploaded to the official NTT DATA website, which clearly outlines the behavior and manners that are taken when communicating with customers. In-house rules have also been defined to ensure that increasingly popular smartphones and tablet devices can be used safely for business. Certain parts of the security rules have been reviewed to ensure that business activities are conducted smoothly.

NTT DATA Information Security Strategies

NTT DATA has defined information security strategies for achieving management policies and minimizing information security risks.

Specific action plans have been established and implemented based on information security strategies.

Risks surrounding management policies and business management

As part of its medium-term management plans, NTT DATA is targeting “Global TOP5” and “Improvements to Corporate Value.”
More specifically, the following three key measures have been put forward as part of medium-term management policies.

- Expanding into new areas, improving product appeal
- Expanding, enhancing and improving global business
- Pursuing overall optimization

Risks related to information security are deemed the risks with the potential for the greatest impact on business management in the medium-term management policy.
The various impacts of information security incidents, including the release or leakage of information are considered the greatest risk, and NTT DATA has focused on guaranteeing information security and protecting personal information as a company that provides information systems.

NTT DATA Information Security Strategies

To better respond to the increasing globalization of customers, the NTT DATA Group has also implemented global management to ensure the spread of knowledge to each and every employee of group companies, and to create a work environment that allows the expertise of the entire group to be applied in full.
The objectives of the NTT DATA Group Security Policy (GSP), ensuring safety of information and actively utilizing and sharing information, are essential as a partner that supports customer reform. More specifically, ensuring the safe distribution of knowledge on a global scale, and implementing efforts for preventing incidents related to information security from occurring are essential for stopping the leakage or release of customer's valuable information.
Each and every employee of the NTT DATA Group is aware of their position as professionals dealing with information, and ensures that information security is always of the highest priority when taking actions.
NTT DATA raised the following three information security strategies in FY2013, and has implemented the necessary measures to achieve them.

■ Information Security Strategies (Objective)

1 Implementing comprehensive recurrence prevention measures

2 Advanced predictor detection and better incident response capabilities

3 Implementing measures to ensure security for commercial systems

4 Increasing security governance

Adoption of Information Security Implementation Policies

Action plans based on information security strategies

NTT DATA's information security policies are developed and implemented in accordance with information security strategies. This page outlines specific action plans for each priority topic raised as part of information security strategies.

Implementing comprehensive recurrence prevention measures

After identifying an incident in November 2012, systems that handle information with a high degree of liquidity that are used by the entire NTT DATA Group were thoroughly inspected, and recurrence prevention measures were applied.

■ **Information security objectives:** a recurrence prevention committee was established immediately after the incident was identified in order to inspect similar systems that are operated throughout the entire NTT DATA Group, as well as develop recurrence prevention measures for reinforcement of access control to key information, early detection of unauthorized access, and personnel management/training. These measures are planned to be implemented thoroughly throughout FY2013.

■ **Action plan:** improving key information management rules, arrangements for ensuring proper operations on site, company-wide management and monitoring, etc.

Advanced predictor detection and better incident response capabilities

There has been an ongoing increase in the number of external threats that cannot be prevented simply by acting carefully – these include increases in targeted cyber-attacks and malware that cannot be detected by anti-virus software.

NTT DATA is working on advanced predictor detection for cyber-attacks, and developing better incident response capabilities.

■ **Information security objectives:** the key objective for FY2012 was the detection of suspicious communications and properly applying security patches.

The objective for FY2013 is to build more advanced detection methods for suspicious communications and to develop better incident response capabilities.

■ **Action plan:** detection with blacklists, detection based on malware infection behavior, creating manuals for incident response, etc.

Implementing measures to ensure security for commercial systems

Cyber-attackers have taken on a more organized manner in recent years, and the methods used have also increased in complexity.

Efforts are being made to ensure better security of commercial systems so that customers using systems provided by NTT DATA can be safe and secure.

■ **Information security objectives:** the objective for FY2012 was to introduce measures for commercial systems aimed at defining “security quality standards” and developing rules for “analyzing serious vulnerabilities.” The objective for FY2013 is to increase deployment of these “security quality standards” and expand the number of systems covered by “analyzing serious vulnerabilities.”

■ **Action plan:** running trials for introducing quality standards, setting up a contact point for analyzing serious vulnerabilities and providing services, monitoring of diagnosis conditions, etc.

Increasing security governance

The NTT DATA Group has formulated a framework for governance designed for operating companies, and efforts are underway for maintaining and improving governance.

■ **Information security objectives:** the objective for FY2012 was to shift to from centralized management to a framework for governance designed for operating companies.

The objective for FY2013 is to identify the current state and issues of operating companies, and provide support for initiatives aimed at maintaining and improving governance.

■ **Action plan:** formulation of framework for security governance and monitoring operations, distributing global information and support for incident response, etc.

Auditing, monitoring

NTT DATA auditing and monitoring system

Internal Audit Department

Auditing details	Conducts information security audits of business departments and group companies.

Information Security Office

Monitoring details	Management objectives have been set for each information security activity, including operating conditions of technical measures, state of establishment of information management systems, and operating conditions of personal information protection. Management conditions are monitored and reported to the CISO. Monitoring of group companies has been expanded from 2011 to cover companies located overseas. The CISO then uses various monitoring results to determine whether information security strategies are being used to achieve management policies, and whether contributions are being made to minimize information security risks.

Improvements to policies based on audit results

Information security audits conducted by NTT DATA are designed to check compliance conditions of information security policies and other regulations. Various types of proposals are also provided to make improvements to activities based on audit results.

Within NTT DATA

Audit results

- Some violations of rules regarding information security were identified.

Proposals

- Further improvements to management as stipulated in regulations are recommended.

Implementing improvements

- Enhance monitoring of audit findings and follow-up on developments through to completion.
- The Audit Division will continue monitoring of the monitoring conditions above, identifying the progress and state of measures for making improvements.

Group Companies

Audit results

- The effects of efforts to make improvements at group companies located overseas have been impressive, leading to a major reduction in flaws.
- Some sections were found to be insufficient with aspects of management stipulated in the Group Security Policy (GSP).

Proposals

- Group companies located overseas are requested to implement more thorough efforts to make improvements.

Implementing improvements

- Develop a security governance system designed for operating companies aimed at faster compliance and response to suit regional characteristics.
- Continue to identify conditions at all group companies through operating companies every quarter, and provide support for improvements as required (share information, discussions, supervised tours etc.).

Information security activity case study 1

Introduction

NTT Data expresses its sincere apologies for the inconvenience caused to victims and all related parties by an incident in November 2012 where an employee at a contracted company acquired cash card transaction information in an unauthorized manner.

NTT DATA implemented appropriate measures faithfully to ensure the safety of important information stored on existing systems.

NTT DATA is taking the fact that this incident could not be prevented very seriously, and is implementing efforts throughout the entire group to develop systems with a high level of security and to improve system operation so that such incidents are not repeated.

Implementing comprehensive recurrence prevention measures

NTT DATA launched a recurrence prevention committee headed by the chief information security officer (CISO), which is in charge of implementing inspections and measures to prevent incidents from recurring within similar systems used throughout all group companies.

Company-wide recurrence prevention measures

■ Reinforcement of management rules for key information

- Clarification of implementation responsibilities for security measures
- Reinforcement of access control for key information
- Early detection of unauthorized access

■ Arrangements for comprehensive on-site operation

- Implementation of training and mental health care from managers (called line-care) for employees and contracted companies
- Consulting of risk analysis
- Organization and deployment of operation case studies and manuals
- Reinforcement of management of contracted companies
- Provision of solution information

■ Company-wide management and monitoring

- Reinforcement of management by designated committee
- Apply knowhow to other business fields

Measures for system developers to prevent internal unauthorized access

■ Thrashing out scenarios of unauthorized access

Instead of focusing solely on actual data, all key information handled by company-wide systems, including those system areas, was identified and every effort made to eliminate scenarios suggesting unauthorized access of key information.

■ Multi-layered protection with prevention, deterrent and detection

To combat potential cases where various measures have been defeated in scenarios of unauthorized access that have been identified, measures for multi-layered protection have been implemented to ensure prevention, deterrent and detection.

■ Review of personnel management

Thorough information security training and line care have been implemented for personnel and cooperating members involved in each project in order to improve the attitudes of each and every employee.

Information security activity case study 2

Early detection of cyber-attacks and better response capabilities for security incidents

Cyber-attacks are becoming more advanced, and include targeted attacks and drive-by downloads. In these types of attacks, attackers use viruses that cannot be detected with anti-virus software, or modify malicious webpages within a short period of time so that URL filters cannot keep up. This makes preventative measures difficult, and thus makes information systems susceptible to such attacks. NTT Data detects advanced attacks at an early stage and responds quickly in order to minimize damage, and every effort is being made to improve incident response capabilities so that a rapid and appropriate response can be provided when security incident occur.

Early stage detection and fast response to cyber-attacks

To defend against advanced cyber-attacks, a multi-layered approach has been taken, which involves input measures, output measures and terminal measures.

As the majority of cyber-attacks exploit known vulnerabilities, protecting devices is possible as long as the latest patches are applied appropriately. As one measure taken to protect such devices, NTT DATA checks the condition of security patches of major software titles, and has introduced a system that does not allow devices that have not been patched properly to connect to the group intranet.

Advanced cyber-attacks that have clearly targeted NTT DATA cannot be adequately stopped by detecting viruses with anti-virus software (input measures) or blocked with URL filters (output measures). To overcome this, NTT DATA conducts R&D on new detection methods and dynamic protection to provide early detection and fast response. Websites related to the NTT DATA Group are regularly monitored to detect an unauthorized modification at an early stage.

Better incident response capabilities

Fast and accurate incident response is required to prevent damage from spreading, to ensure that systems are restored quickly and to prevent recurrence of such incidents. This type of incident response calls for an extremely advanced skillset, including instructions for external response, forensics (chasing trails), identifying the extent of damage and causal analysis.

To combat this, NTT DATA is working at increasing the skills of NTTDATA-CERT members, specialists when it comes to incident response.

Response training for targeted attacks run for management level employees in FY2011 was expanded to include ordinary employees in FY2012. This training was run so that employees were capable of providing initial response in accordance with the guidebook outlining measures against targeted attacks.

NTT DATA also participated in joint incident response drills run by the NTT Group to ensure an appropriate response in the event that an information security incident does occur. Mock training was conducted here, from identifying the conditions behind an information security incident through to restoration.

■ Scene from incident response drills run by the NTT Group

Information security activity case study 3

Implementing measures to ensure security for commercial systems

The level of damage from incidents such as leakages of personal or confidential information, or business downtime has increased in recent years as a result of unauthorized access resulting from insufficient security (vulnerabilities) of information systems. NTT DATA is taking steps to propose the most appropriate security measures for customer information systems or services based on the latest security data and technical trends to combat threats related to unauthorized access.

The first step is to examine systems in their entirety for existing vulnerabilities that could be expected to cause major damage. With this in mind, effective security improvement measures are being proposed to suit the characteristics of information or business handled by systems, as well as customer requests.

In the NTT DATA Group, the business division works closely with the Information Security Office, the technical development division and group companies related to security to implement various types of initiatives in order to provide all customers with appropriate security solutions.

Responding to the latest trends in security technology

The required level of security measures in commercial systems provided to customers varies depending on information being handled, business or system type or architecture in use. Measures based on the latest technical trends are also required for the latest system framework technology that is constantly evolving.

The NTT DATA Group shares information on the latest security technical trends and vulnerabilities throughout the group, and is also developing a framework for ensuring the required security level for systems being built by incorporating examination processes to ensure security as part of standard company-wide processes for system development and operation. Developed systems are also regularly diagnosed for security flaws by experts, and if newly identified vulnerabilities arise, the appropriate measures are put in place. This ensures that customers are continually provided with safe and secure systems and services.

Customers in the social infrastructure, financial and a wide range of industries demand core systems that are protected with even more advanced security. For these systems, the business division and R&D division of both NTT DATA and NTT Group work together for technical development to provide advanced security solutions that are one step ahead of the latest security technology in a timely manner.

Establishment of the “Forensic Laboratory”* organization specializing in the digital forensics field

Work involved with conventional security measures have focused on just how well they can prevent incidents such as unauthorized access from occurring. Yet the advances being made to methods used to conduct cyber-attacks in recent years have made it difficult to notice that damage has even been inflicted, or even identify the type of damage. This increases the time required for restoration, introducing the issue of increased damages or opportunity loss. And completely preventing internal fraud that utilizes authorized access is difficult, however it has become vital to take measures that can detect incidents quickly and ensure recovery, as well as to prevent them from recurring, rather than relying on measures that are aimed at convention forms of protection.

With these types of changes occurring in the security-environment, there are calls for security measures that utilize digital forensic technology involving identifying the causes of incidents, the extent of damage or impact, as well as conserving trails that may suggest cyber-attacks and unauthorized access.

In October 2013, the NTT DATA Group established the “Forensic Laboratory” organization specializing in pioneering R&D in the field of digital forensics in order to meet these growing needs. The “Forensic Laboratory” focuses on technical development related to forensics, malware analysis, cyber-attacks and early detection of internal fraud, as well as provides training for personnel utilizing these technologies.

* The Forensic Laboratory is made up of System Platforms Sector, IT Security Business Section.

Information security activity case study 4

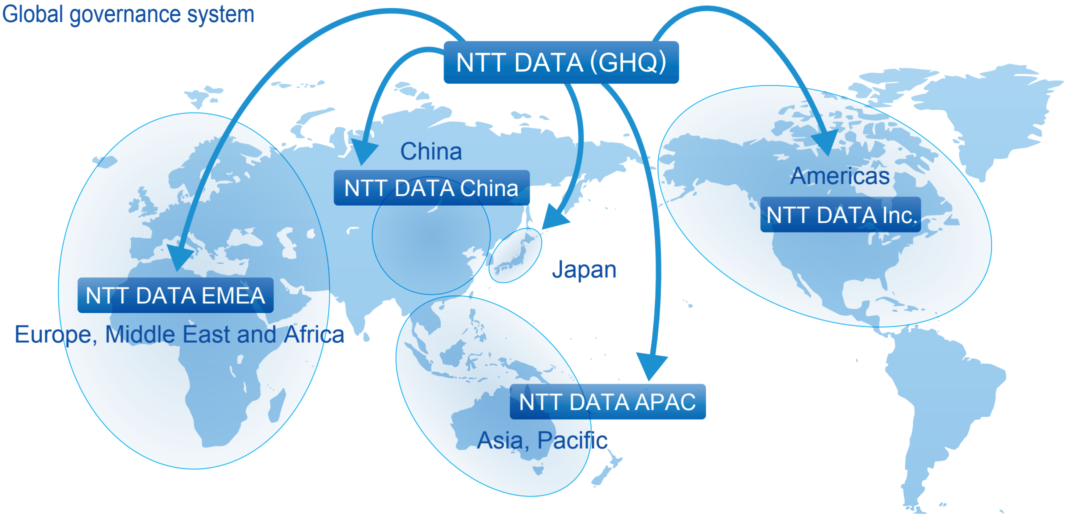
Full-scale global deployment

The NTT DATA Group has run its business management based on five main regions around the world [Americas, EMEA (Europe, Middle East, and Africa), APAC (Asia, Pacific), China and Japan] and solutions since FY2012. It has redeveloped an operating system for information security with operating companies at its core in line with this.

In FY2013, a security policy has been developed centered on operating companies based on the GSP (NTT DATA Group Security Policy), and started operation of security at the regional and business level. This has led to a shift from a governance system where group companies and NTT DATA work one-on-one, to a system run by operating companies to suit regional characteristics and allow faster response times.

Each solution calls for the operation of security governance in line with regional characteristics.

■ Global governance system



Increased level of security governance operation

The operating companies are maintaining PDCA cycles (establishing rules and promotional systems, organizing management and running education and training, checks with internal audits). NTT DATA monitors the management conditions of each operating company every quarter in order to identify issues. Support for improvements is provided to maintain and increase management levels through initiatives such as sharing information, holding discussions, and organizing supervised tours.

Distributing global information and incident response

NTTDATA-CERT has built a collaborative system with security officers at each operating company. It also provides knowhow on incident response to those operating companies.

Operating companies approach NTTDATA-CERT for holding discussions related to security incident response.

Information on vulnerabilities provided to NTT DATA and group companies in Japan are also provided to group companies located overseas in order to develop a system that is capable of responding quicker security threats affecting the entire NTT DATA Group.

Improving understanding and awareness of information security

Continuous information security training and education

The NTT DATA Group is aware that each and every executive, employee and partner is a professional dealing with information, and always considers information security policies during daily actions to ensure continuing information security.

NTT DATA focuses on improving understanding of rules and actions, and takes the appropriate steps for employees to develop an information security-minded approach required for work by adopting ongoing information security training and educational activities.

Information Security Training

The NTT DATA Group has conducted ongoing information security training to ensure that employees gain an understanding of the need for the protection of personal information and rules outlining group security policies, as well as ensuring that they act with a full awareness of information security.

■ Information security training records at NTT DATA in FY2012 and FY2013

Applicable to	Type of Training	Details, Objectives
All employees (required)	Personal information protection IBT (Web interface)	Approach to personal information / Methods for dealing with personal information / Understanding the details of company regulations / Increasing awareness of personal information * Records for FY2012, FY2013: employees 100%
	Information Security Policy Assessment (Web interface)	Increasing awareness of information security policies / Understanding of basic actions in the event of an information security incident / Dealing appropriately with cell phones and small portable media etc, acquiring correct knowledge * Records for FY2012, FY2013: executives, employees 100%
All employees (optional)	Information Security Workshop	Workshop designed around the items that receive a large number of inquiries related to information security and protection of personal information * Records for FY2012: 6 times, FY2013:3 times
All employees (per work group, optional)	"Information Security ABCD Activities" case study	A group discussion venue focusing on thinking for yourself for gaining a better under-standing and penetration of information security measures Conducted at each workplace based on case studies of actual near-misses
Each management level	Information Security Course (classroom training)	Description of the knowledge, differences in roles and responsibilities, approach, and required items for each employment position, including new employees, mid-career employees, division managers, and department managers Acquiring knowledge for improving understanding and implementation of information security
Partners (required)	Personal Information Protection In troduction Training Information Security Training (Web interface, provision of training materials)	Provides training of content that should be known by partners working at NTT DATA related to the protection of personal information, and information security rules at NTT DATA Training is required when using company systems, and regularly training is essential * Available in multilingual format (English, Japanese, Chinese)
Partners (new partners)	Information Security Training Handbook	Handbook that outlines how to deal with information security and personal information when working within the NTT DATA, distributed by contract from the NTT DATA Group. The handbook is for new NTT DATA Group partners. * Available in multilingual format (English, Japanese, Chinese)

Supporting group company educational activities

NTT DATA provides the required tools and support required by each group company to develop their own information security training with a view of improving the level of information security throughout the entire group, and to apply the "PDCA Double Loop" concept designed specifically with globalization and group expansion in mind.

■ Group company training support tool

Applicable to	Type of Training	Details, Objectives
Group Company Employees	GSP security training (Web interface)	Improving NTT DATA Group Security Policy understanding / Methods to deal with personal information / Description of the NTT DATA Group Security Policy * Available in multilingual format (English, Japanese, Chinese) * Records for FY2012: 80 companies, 26,129 employees, FY2013: 87 companies, 28,152 employees
Group Company Partners	GSP Security Training for partners (Web interface)	Approach related to personal information protection, training for information security rules that should be known as new NTT DATA Group partners * Started in FY2012: 65 companies, 22,995 employees, FY2013: planned on Febrary, 2014
Internal Auditors	GSP Internal Auditor Training (Offline training)	Training for conducting information security audits Training with simulated audits * Available in a multilingual (English, Chinese, Japanese) format that can be completed by employees at their desks * Records for FY2012: 61 companies, 156 employees, FY2013: 83 companies, 347 employees

Examples of information security promotional tools

In addition to focusing on the basic security activities that have been raised as priority topics as part of information security strategies, NTT DATA also conducts ongoing information security educational activities with the aim of maintain and increasing the level of information security.

■ Information security promotional posters

Topic for FY2012

Check rules for smartphones and tablet devices/Defend yourself against targeted attacks

NTT DATA
Defend yourself against targeted attacks!
Information Security
Check Your Security Status

Posters are designed on recent topics such as world and social trends and priority topics of information security strategies, and help to better identify information security within each workplace. A multilingual version started being issued from FY2008 and is released to other group companies.

■ Monthly newsletter "Security Today"

Outlines the efforts taken within the NTT DATA Group for information security, social condition related to security, the most recent technology, and reports of incidents in an email magazine that is published monthly.

Part of the newsletter is provided to group companies and partners to share information.

■ Message from CISO

From FY2011, CISO will be sending messages directly to employees once per quarter. This can be used as an opportunity for CISO and employees to interact, via reports on the latest trends, approaches taken by CISO, and requests for employees.

Efforts taken by contractors

NTT DATA has developed various standards to prevent the unexpected leakage or release of information from partner companies contracted to develop software. When contracting work that deals with confidential information or personal information, declarations are received, and checks conducted of security response conditions being taken.

Partner company selection

Checks of system and response conditions

To select clients that meet certain standards, a different set of standards is defined and the client interviewed to check their current security response conditions.

Present rules, agree on response rules

Present rules related to security management and protection of personal information required for a particular project, and reach an agreement on the level of response required by the partner company.

Efforts after business contracts

Start contract

Training, check declarations

- Provide training to partner companies dealing with information in line with the details agreed upon during the contract.
- Check and receive copy of declarations.

Report from partner company

Information management systems, conditions for dealing with information, and security response conditions are checked regularly using submitted reports or meetings that are held.

Audit of partner company

On-site or other inspections may be conducted if required to check security response conditions, and to determine whether information is being operated and managed appropriately. Requests for corrections or improvements may be issued depending on the results.

Check of information disposal

Information that is no longer required for its original purpose, information that is in use but no longer required, or media storing this type of information must be returned or destroyed using the methods stipulated in advance by the project.

End contract

Third party assessments, certification

ISMS certification acquisition conditions

Where required, NTT DATA and NTT DATA Group companies have acquired international standard ISMS (ISO/IEC 27001) certification for information security management system when dealing with confidential information or personal information.

Group companies with organizations that have acquired ISMS certification are as follows. (41 companies including NTT DATA, as of the end of December 2013)

■Companies with groups that have acquired ISMS Certification

NTT DATA Corporation	NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc.	NTT DATA SEKISUI SYSTEMS Corporation
NTT DATA SYSTEM TECHNOLOGIES Inc.	NTT DATA SMS Corporation	NTT DATA TERANOS Corporation
NTT DATA i Corporation	NTTDATA CUSTOMER SERVICE Corporation	NTT DATA NCB Corporation
NTT DATA INTELLILINK Corporation	NTT DATA FORCE CO., LTD.	NTT DATA Getronics Corporation
NTT DATA FINANCIAL CORE Corporation	NTT DATA FRONTIER Corporation	NTT DATA CCS Corporation
NTT DATA HOKKAIDO Corporation	Realize Corporation	NTT DATA MSE Corporation
NTT DATA TOHOKU Corporation	NTT DATA Smart Sourcing Corporation	JSOL Corporation
NTT DATA SHINETSU Corporation	NTT DATA WAVE Corporation	NTT DATA ITECS Corporation
NTT DATA TOKAI Corporation	NTT DATA CHINA OUTSOURCING Corporation	NJK Corporation
NTTDATA HOKURIKU Corporation	NTT DATA BUSINESS BRAINS Corporation	NTT DATA MCS Corporation
NTT DATA KANSAI Corporation	NTT DATA SOFIA Corporation	EMAS Co.,Ltd.
NTT DATA CHUGOKU Corporation	QUNIE Corporation	Japan Information Processing Service Co., Ltd.
NTTDATA SHIKOKU Corporation	NTT DATA BUSINESS SYSTEMS Corporation	NTT DATA Financial Solutions Corporation
NTT DATA KYUSHU Corporation	Technology Power Corporation	

Privacy Mark Registrations

Companies under NTT DATA or the NTT DATA Group that have been registrated the Privacy Mark are as follows. (34 companies including NTT DATA, as of the end of December 2013)

■Group companies registrated with a Privacy Mark

NTT DATA Corporation	NTT DATA SMS Corporation	Technology Power Corporation	NTT DATA ITECS Corporation
NTT DATA i Corporation	NTTDATA CUSTOMER SERVICE Corporation	NTT DATA SEKISUI SYSTEMS Corporation	TOUHOKU INFORMATION SYSTEM CO.,LTD.
NTT DATA INTELLILINK Corporation	NTT DATA MANAGEMENT SERVICE Corporation	NTT DATA SMIS CO., Ltd.	Media Drive Corporation
NTT DATA HOKKAIDO Corporation	NTT DATA FRONTIER Corporation	NTT DATA ENGINEERING SYSTEMS Corporation	EMAS Co., Ltd.
NTT DATA TOHOKU Corporation	NTT DATA UNIVERSITY Corporation	NTT DATA TERANOS Corporation	NTT DATA BEEN Co., Ltd.
NTT DATA TOKAI Corporation	NTT DATA Smart Sourcing Corporation	NTT DATA CCS Corporation	Japan Information Processing Service Co., Ltd.
NTT DATA KANSAI Corporation	NTT DATA ABIC Co., Ltd.	JSOL Corporation	Integrate System Service Co.,Ltd.
NTT DATA CHUGOKU Corporation	NTT DATA WAVE Corporation	XNET Corporation	JSF INFORMATION TECHNOLOGY CO., LTD.
NTT DATA INSTITUTE OF MANAGEMENT CONSULTING, Inc.	NTT DATA BUSINESS SYSTEMS Corporation		

Information security activity timeline

	Social Developments	Technical Developments	NTT DATA Achievements, Developments
1998			**December** "Information Security Policy" developed
2000	**July** Developed JIS X 5070, the Japanese version of ISO15408 International standards for information security **September** BS7799 Part 1 became International Standards ISO/IEC17799	Google (Japanese) started operations Increase in DoS attacks **October** "WinMX" Beta version released **December** NTT East and West "Flet's ADSL" started	**February** Greater venture systems (NTT DATA INTRAMART CORPORATION established) **March** Accounting system using consolidated balance sheets started from the March quarter **June** Information security policy assessments started
2001	e-Japan strategy developed	AES selected as the American government's standard encryption service to replace DES and triple DES "Code Red" and "Sircam" worms spread **June** NTT East and West "B Flet's" started **November** First person arrested for using "WinMX"	**February** "Standard Security Policy (SSP)" developed **June** "Personal Information Protection Regulations" developed **July** "Personal Information Protection Policy" announced **September** First BS7799 certified in Japan
2002	**April** Started operation of the ISMS Conformity Assessment Scheme from Japan Information Processing Development Corporation (JIPDEC)	Botnet appeared **May** P2P software "Winny" Beta version released	**September** Training (CISP) started for partners **October** NTT DATA Group Security Agreement (GSA) established
2003	**October** Japan Information Security Audit Association established	Skype established **January** "Slammer" worm spread **August** Skype public Beta version released	**June** Acquired Privacy Mark Certification **July** Established system for regional subsidiaries (system incorporating nine regional subsidiaries)
2004	Google stocks went public	**January** "Share" released **February** "W32/Netsky" worm spread **May** Developer of P2P software "Winny" arrested	
2005	"Web 2.0" became popular **April** Personal Information Protection Law enacted in full	**December** "Youtube" service officially started	**June** P2P software checks became available for remote connection PCs **November** Started TSF operation
2006	Numerous cases of information leakage reported due to file sharing software "Winny" **February** "Information Security Day" established	"Facebook" released to the public **July** "Twitter" service started operations **December** "Amazon EC2" started, kicking off the cloud computing concept **December** Domestic high-speed PLC products went on sale	**July** Started trials of Telework **September** Declaration received from all Employees at NTT DATA (ensuring that users delete work related information from their own PCs, and prohibiting work on their own PCs) **October** Declarations required from all Employees working within the NTT DATA Group **November** Declarations required from subcontractors
2007	**January** "Information Security Governance Seminar" held	**October** The number of Skype online users exceeded 10 million people	**April** ISMI Certification obtained for the head office building **July** Thin client services started **December** Email filtering service started
2008	**January** First person arrested in Japan for creating computer virus **June** National Information Security Center (NISC) released "Secure Japan 2008"	**February** Virus found to spread via USB memory **April** Google and Salesforce.com announced tie-up for cloud computing	**February** Telework system started **March** First "2008 Information Security Report" as system integrator published **April** NTT DATA Group Security Policy (GSP) published **November** "Information Security Improvement Month" established
2009	**February** NISC released "2nd Information Security Basic Plan" **June** NISC announced "Secure Japan 2009" **September** Personal Information Protection Law shifted to the Consumer Affairs Agency	**April** "Gumblar" botnet appeared	"Secure Friday" established **December** Comprehensive cloud solution service announced

	Social Developments	Technical Developments	NTT DATA Achievements, Developments
2010	**July** Information Security Policy Council released "Information Security 2010" **July** Unfair Competition Prevention Act revised **November** Video of Chinese boat collision incident leaked	Widespread attacks targeted Twitter **May** iPad released in Japan **December** First botnet virus "Geinimi" for Android appeared	**March** "2010 Information Security Report" published **July** "7 Wise Conditions for Basic Security Activities" established **July** NTTDATA-CERT established
2011	**March** Widespread fishing scams reported in the aftermath of the Great East Japan Earthquake **May** Vast amounts of personal information leaked from American subsidiaries of Japanese companies due to cyber attacks **June** "Virus Creation" is criminalized following revisions to criminal law **September** Targeted attacks discovered against the Japanese defense industry	**May** IPv4 addresses depleted in the Asia Pacific region **June** Numerous cases of damage from internet banking transactions due to SpyEye	**April** Joined NTTDATA-CERT FIRST **May** Internal connection service for smartphones started **June** NTT DATA Social Media Policy announced **July** Office computers switched to notebook PCs following restrictions to power consumption
2012	**March** Act on Prohibition of Unauthorized Computer Access revised **April** Initiative for Cyber Security Information sharing Partnership of Japan (J-CISP) started **June** “Act to revise part of the Copyright Act” enacted to criminalize illegal downloads **November** “Convention on Cybercrime” became effective in Japan	**June** Firstserver, Inc. lost large amounts of stored companies’ data **October** Damage incurred and number of cases increased from internet banking virus targeting Japanese banks	**February** Training for targeted email attacks (for executives and management level) **March** “Information Security Report 2012” issued **July** Training for targeted email attacks (for employees)
2013	**May** “Act on the use of the number to identify a specific individual in administrative procedures” (My Number Act) established **June** Information Security Policy Council released “Cybersecurity strategy” **July** OECD privacy guidelines revised **October** ISO/IEC27001 revised	**March** Cryptography Research and Evaluation Committees (CRYPTREC) released “e-Government Recommended Ciphers List”	**April** New governance system run by operating companies started **June** Online storage service application system introduced **October** “Forensic Laboratory” established

■ Participating groups (excerpt)

- Japan Information Technology Service Industry Association
- Japan Information Processing Development Center
- Japan Information Security Management Systems User Group
- FIRST(Forum of Incident Response and Security Teams)
- Nippon CSIRT Association
- Japan Society of Security Management
- Japan Network Security Association
- The Institute of Digital Forensics
- Japan Information Security Audit Association
- The Japan Society of Information and Communication Research
- The Institute of Electronics, Information and Communication Engineers
- The Society of Project Management
- Union of Japanese Scientists and Engineers
- The Japanese Society for Quality Control
- Next Generation IP Network Promotion Forum
- Internet Protocol Data Cast Forum
- Cloud Utilization Promotion Agency
- Information Security Technology Study Group
- Japan Image and Information Management Association
- Security Promotion Realizing sEcurity meAsures Distribution(SPREAD)
- Japan Users Association of Information Systems
- The Telecommunication Technology Committee
- Electronic Commerce Security Technology Research Association
- IC System Security Round Table
- Japan Multi-Payment Network Promotion Association
- Ic Cashcard Type Approval Council
- Japan IC Card System APplication council(JICSAP)
- IT Coordinators Association
- Software Engineers Association
- Japan Telework Association

Other

Company overview

Ever since separating from Nippon Telegraph and Telephone Public Corporation in 1988, the NTT DATA Group has been providing information systems and services to address the requirements and issues of society. The company is involved with systems for public services, finance, manufacturing, logistics, communications, medical, health care and other corporate-oriented systems, as well as social infrastructure services that cover multiple industries.

Today, NTT DATA is focusing its resources on globalization, and has expanded its offices located in 141 cities, in 34 countries as of September 30, 2013.

As a company that is truly pioneering the IT industry in Japan, and a company that has a global presence with businesses operating in every region on the planet, there are plans to provide further support to society and develop new frameworks and value required for reforms.

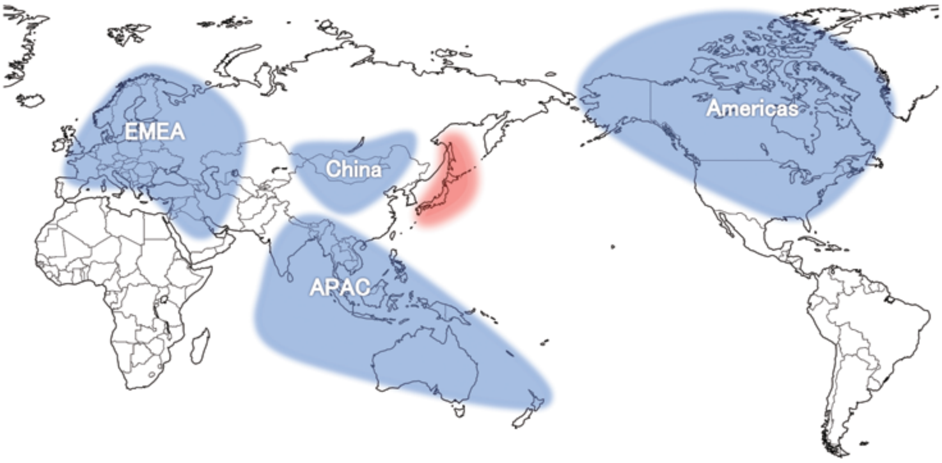
Name	NTT DATA CORPORATION
Head Office	Toyosu Center Building, 3-3, Toyosu 3-chome, Koto-ku, Tokyo 135-6033, Japan
Established	May 23, 1988
President and CEO	Toshio Iwamoto, President and Chief Executive Officer
Common Stock	142,520 million yen (as of March 31, 2013)
Net Sales (consolidated)	1,301,900 million yen (April 1, 2012 to March 31 2013)
Ordinary Income (consolidated)	81,870 million yen (April 1, 2012 to March 31 2013)
Number of Employees (non-consolidated)	10,804 (as of March 31, 2013)
Number of Employees (consolidated)	61,369 (as of March 31, 2013)
Subsidiaries and affiliated companies	Consolidated subsidiaries: 217 (as of March 31, 2013) Affiliated companies: 18 (as of March 31, 2013)
Business Areas	System integration/Networking system services Other business activities related to the above
State of Global Offices	

Europe, Middle East, Africa
59 cities
6,600 Employees

Asia Pacific
22 cities
10,700 Employees

China
13 cities
4,400 Employees

Americas
47 cities
7,400 Employees



* No. of Employees as of September 30, 2013

Implementation of information security as a corporate group

In closing

The environment that companies operate in is constantly evolving, and the risks associated with information security are become more advanced and more diversified, resulting in a greater level of damage.

Targeted attacks have a major impact on society. DDoS attacks, manipulation of websites and leakage of information also occur with great frequency. Incidents involving information security has spread to every corner of the IT services industry, with examples including the theft of personal information from unauthorized applications installed on smartphones, increased damage due to unauthorized access from passwords being shared around the internet, or cloud service operates losing customer data. NTT DATA continues to propose information security measures that meet with this changing environment without making any compromises.

The NTT DATA Group information security governance also takes on a governance system run by operating companies, with regional security policies based on the GSP (NTT DATA Group Security Policy) for each of the five regions and solutions (Japan, EMEA, APAC, China, Americas, and Solutions) developed and put into operation. This has allowed information security of the NTT DATA Group to be managed quicker and more accurately. NTT DATA and these operating companies work closely together as NTT DATA provides security information, while each operating company holds discussions on incident response and reports on progress related to information security.

The NTT DATA Group will continue to take steady and focused efforts for implementing information security. This is because each and every employee of the NTT DATA Group considers themselves a professional handling information, and always takes action with an awareness of information security. In turn, this helps to increase customer satisfaction levels and information security capabilities within the NTT DATA Group.

As a corporate group working at the core of IT society, NTT DATA will continue its efforts in implementing further information security to provide customers with a new sense of value with safe and secure services, all without betraying the customer.

NTT DATA Corporation
Manager, Information Security Office,
Quality Assurance Department
Shigefumi Takahashi

NTT DATA Group Information Security Report 2014
Published by: Information Security Office, NTT DATA CORPORATION

Issue Version 1.0 March 2014

Note: Service, product and other names listed in this report are registered trademarks or trademarks of NTT DATA or their respective owners.

NTT DATA Corporation
Toyosu Center Bldg., 3-3, Toyosu 3-chome,
Koto-ku, Tokyo 135-6033, Japan
Tel: 03-5546 8051 (switchboard)
www.nttdata.com